Advanced Security for your Cloud

Public, Private, Hybrid, and Multi

Evan Dumas | Regional Director - SEA

Check Point
SOFTWARE TECHNOLOGIES LTD.

Cloud Threat Landscape

"Cloud workloads have become a major attack vector"

"Cloud providers are not responsible for securing your data"

14.3.2018 LA County 211 service , a non-profit organization in Los Angeles County misconfigured an Amazon Web Services (AWS) S3 cloud bucket — leaving 3 million records and highly sensitive health information exposed

30.9.2018 50 Million Facebook Accounts Exposed to Takeover in Huge Breach

1.12.2014 SEC issues $35 million fine over Yahoo failing to disclose data breach (online email service hack)

Thailand, March 2018: True Corp's data gaffe

In March 2018 security researcher Niall Merrigan revealed that the identity

Singapore, September 2017: Reputation debacle for AXA Insurance and Uber

And in December, just a couple of months after AXA's episode, Uber disclosed that personal data belonging to 380,000 of its customers in Singapore had been subject to a leak the previous year.

The popular but controversial riding company only released the news after disclosing that the details of 57 million worldwide Uber riders and drivers had been exposed. Not only that, Uber paid $100,000 to the hacker responsible to destroy the data in an effort to cover up the leak.

but there was no security on the data bucket and anybody could have found and downloaded the files.

Who are the stakeholders for Cloud Security?

Developer

1. Use certified open source
2. Use harden OS / Container
3. Static / Dynamic code analysis

DevOps

1. Labeling workloads
2. Define micro-segmentation
3. Define security during dev cycle (Dev, QA, Staging, Production)
4. Following compliance guidelines
5. Deploy security blueprint

IT Security

1. Define guidelines
2. Securely connectivity
3. Define N/S Access Control
4. Define Macro segmentation
5. Apply threat prevention
6. Monitor compliance
7. Incident response

Traditional Datacenter vs. Cloud

Check Point
SOFTWARE TECHNOLOGIES LTD.

COMPLEX

CLOUD

- Cloud applications and infrastructure
- Deployed by **multiple teams** not under IT control
- High likelihood of inconsistencies and misconfigurations

SIMPLE

TRADITIONAL DATA CENTER

- On-premises infrastructure and applications
- Deployed by highly trained teams
- Tight control over security and compliance

Security Challenges in the Cloud



Infrastructure Challenges

- Shared Responsibility
- Minimal Visibility
- Ever-Changing workloads
- Multi-Cloud

Internal Risks

- Misconfigurations
- Insider Threat
- Compliance and Regulations

External Threats

- Malware
- Zero-day Threats
- Account Takeover
- Gen V Attacks

Shared Responsibility

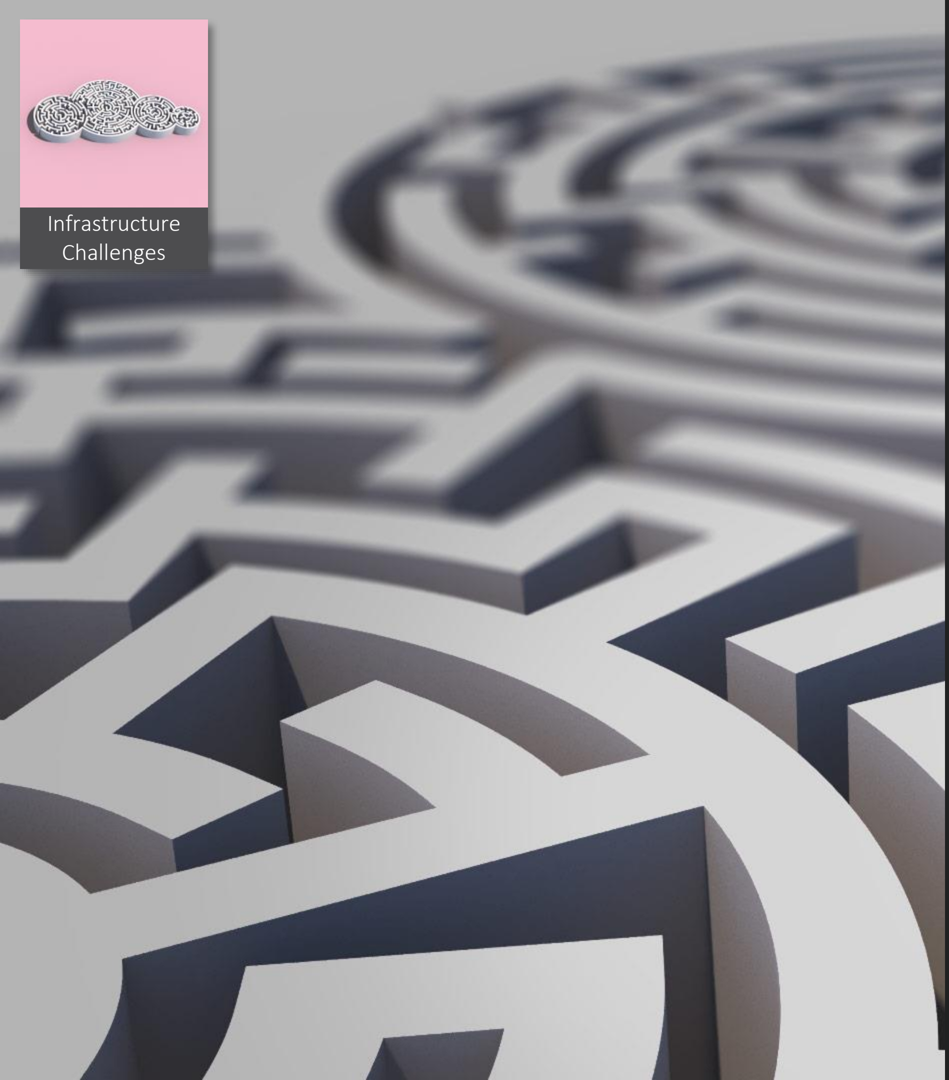
- Cloud providers protect Infrastructure
- Companies must protect Cloud Workloads

Provider Responsibility

Hardware, SDN, Networking, Internet connection

Customer Responsibility

Application code, Application Data, Application Access, Compliance



Minimal Visibility

Check Point
SOFTWARE TECHNOLOGIES LTD.

- Cloud deployments result in challenges around identifying and quantifying assets
- Invisible and unmanaged assets create large gaps in security enforcement

> *"Organizations … are struggling with visibility, making it almost impossible to determine what computing tasks are taking place where, under whose direction."*

Hype Cycle for Cloud Security, Gartner, 7/2018

Ever-changing Workloads

- Cloud assets are provisioned and decommissioned dynamically in large scale and fast pace
- Traditional security tools were not developed for the cloud and thus cannot enforce policies in such a flexible environment
- Traditional security can’t work with orchestration tools

> “*Cloud computing is dynamic, with workloads spinning up and spooling down. unprepared organizations are finding that active enforcement of policy becomes increasingly impractical.*”

Hype Cycle for Cloud Security, Gartner, 7/2018

Multi Cloud

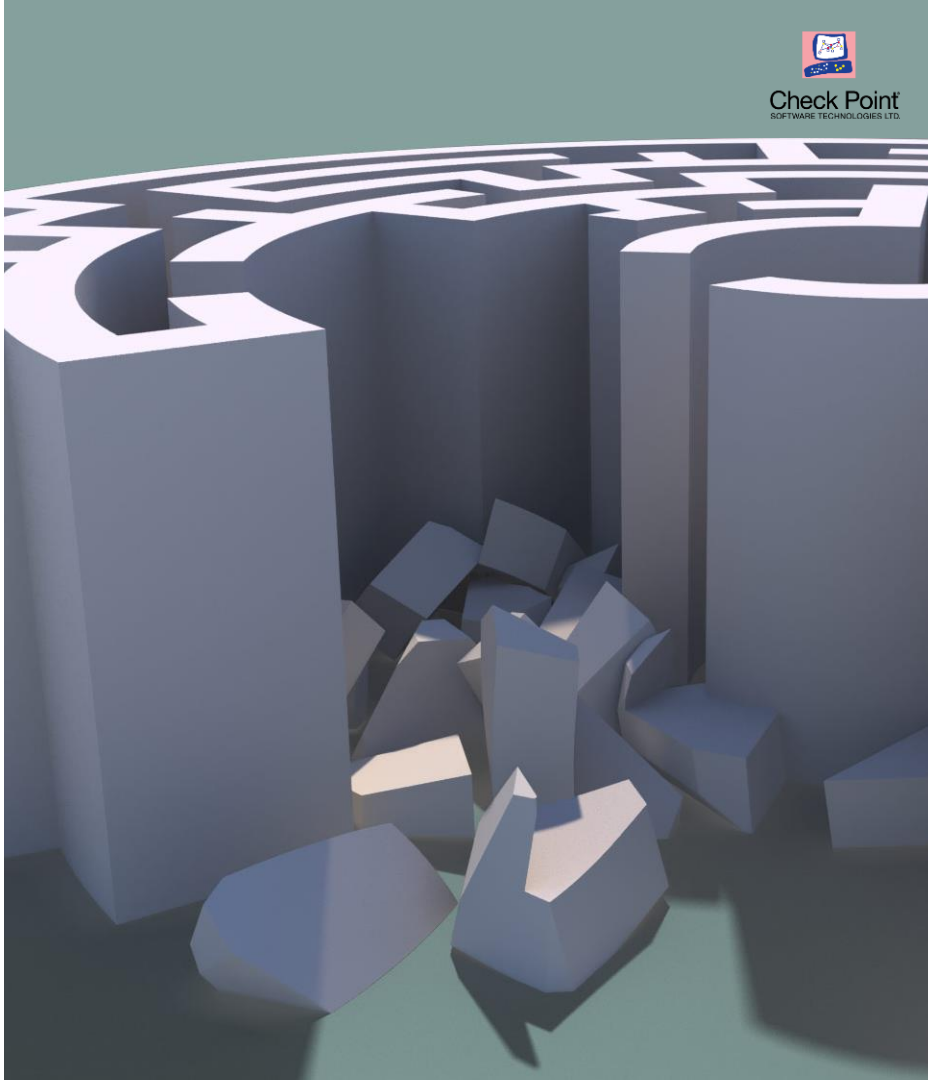
Manageability
Relying on the native security controls of the cloud providers limits the ability to manage security in multi-cloud with a unified tool

Complexity
Difficult to detect and prevent attacks across distributed applications

Consistency
Security posture and governance policies are not consistently applied across on-premises datacenters and cloud providers

Flexibility
Cloud environments cannot simultaneously change and apply the security enforcement in real-time

Internal Risks



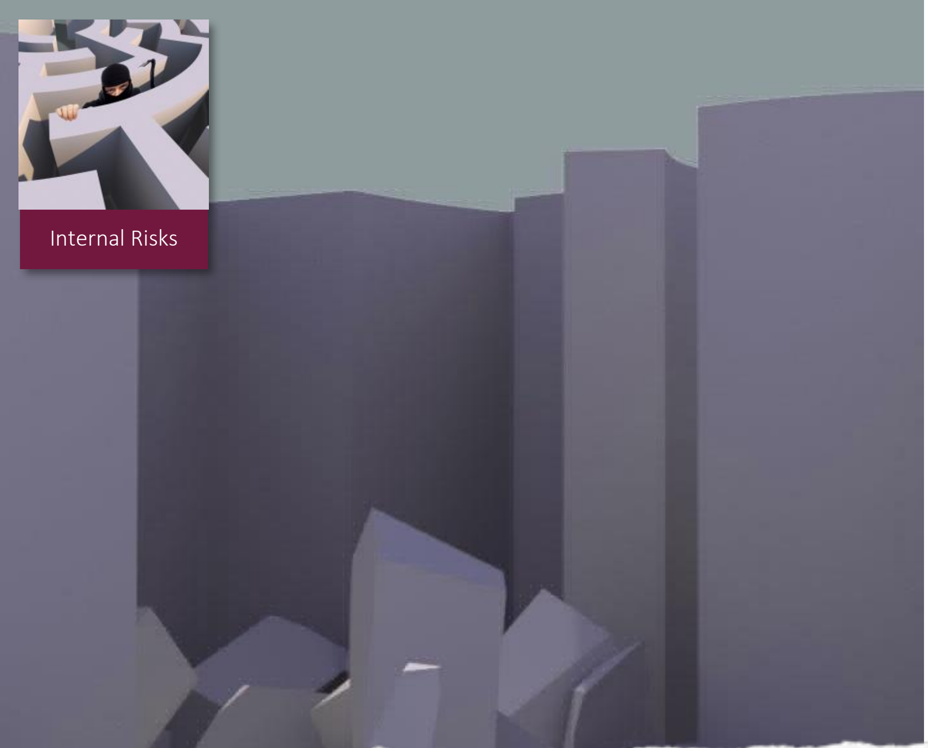
Misconfigurations

Most of the stolen data incidents in the cloud are related to simple human errors rather than concerted attacks

> “*Through 2020, 95% of cloud security failures will be the customer’s fault*”

Gartner

Is the Cloud Secure?
March, 2018



Misconfigurations

Common examples are:

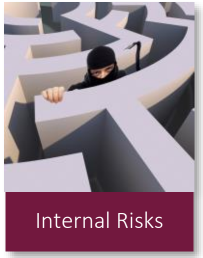
- Over permissive access configuration to services
- Weak administrative user passwords
- No governance over cloud services and API usage

DARK Reading

Jun 1 2018 **10,000** businesses are affected by a widespread misconfiguration in Google Groups settings

Insider Threat

- Rouge employees, disgruntled or recurred by attacker can leverage misconfigurations to create massive damages.
- An administrator with access to the root account of a cloud service can easily duplicate this info to other places.
- Companies are saving source code on external repositories, such as GitHub, with no access restrictions essentially open for all.
- A worker with high-level IT access privileges can load Bitcoin mining software onto the cloud workload



Compliance & Regulations

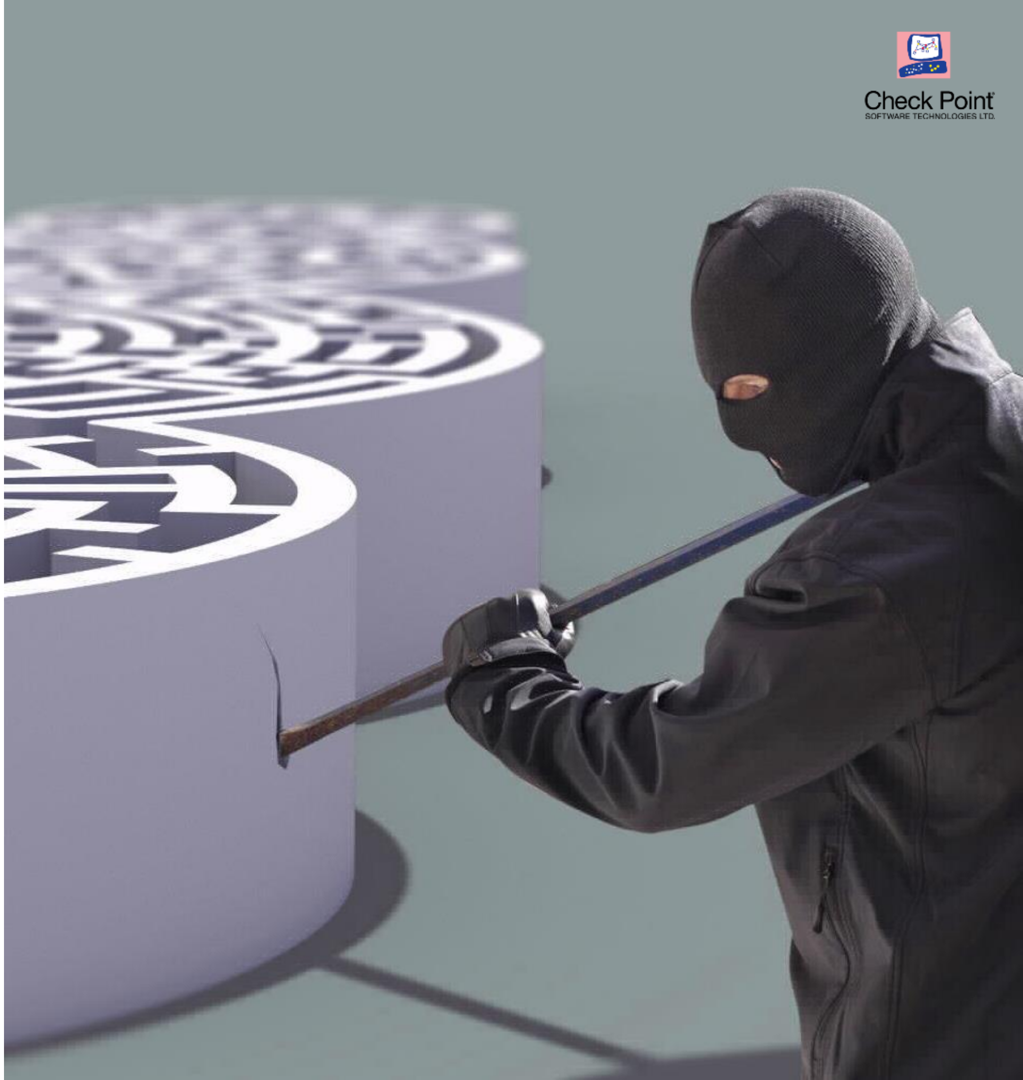
+ Compliance & self governance are highly focused areas for companies in regulated industries (HIPAA, PCI-DSS) or in certain geographical areas (GDPR)

+ Lack of visibility, the dynamic nature of cloud and lack of certainty regarding the location of the payload, all make compliance a challenging task.

External Threats

Zero-day

- Attackers are targeting cloud workloads because they can be accessed via the internet and not hidden inside the on-premises LAN
- Thru lateral movements, once an asset gets infected, both the cloud and On-premises infrastructures are at risk (the cloud can be a bridge to the on-premises datacenter)
- The cloud is a company’s new data center. It is exposed to the same threats as the on-premises data center and possibly even more, such as: Worms / Crypto locker / Bot attacks



Check Point
SOFTWARE TECHNOLOGIES LTD.

Top 5 Cloud Security Design Guidelines

1. Protecting all assets
VM, Container, Serverless, PaaS , Apps, Network, Repositories

2. All Disciplines
Hardening, Compliance, Access, Threats, DLP

3. Enabling DevOps & IT
Automated Deployment , Adaptive Policy, API deployment

4. Secure all Clouds
AWS, Azure, Google, Ali, OCI, Private NSX, ACI

5. Leveraging Native controls
Logs, Controls, Remediation, Orchestration

Rethink Your Security

- Changing the way security is implemented in the cloud
- Security that is more flexible and agile
- Security that enables the business
- Security that prevents advanced threats

CloudGuard Suite

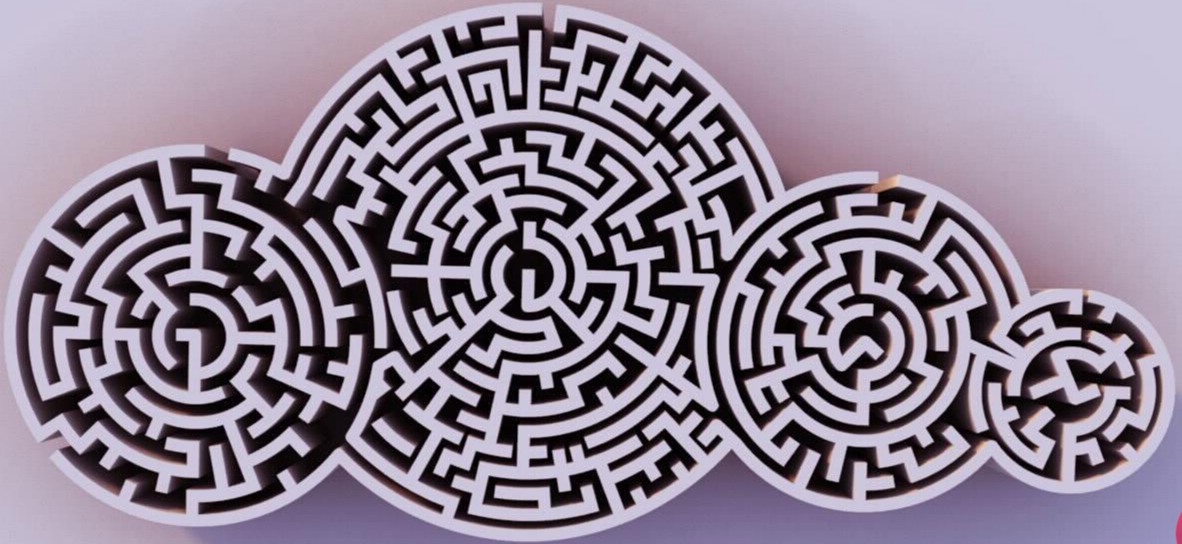
Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT CloudGuard SaaS

Preventing attacks on SaaS applications and cloud-based email

CHECK POINT CloudGuard Dome9

Visibility, compliance and governance, network security



CHECK POINT CloudGuard IaaS

Public Cloud - Access control and advanced threat prevention

CHECK POINT CloudGuard IaaS

Controller - Adaptive security for all major cloud providers

CHECK POINT CloudGuard IaaS

Private Cloud - Advanced threat prevention for East-West and North-South traffic

CloudGuard Suite

Public Cloud

- Advanced threat prevention to all cloud workloads, including: IPS, Anti-Bot, Sandboxing and access control
- Unified award winning management system managing all cloud environments
- Micro segmentation – full control over East-West traffic (lateral movements)

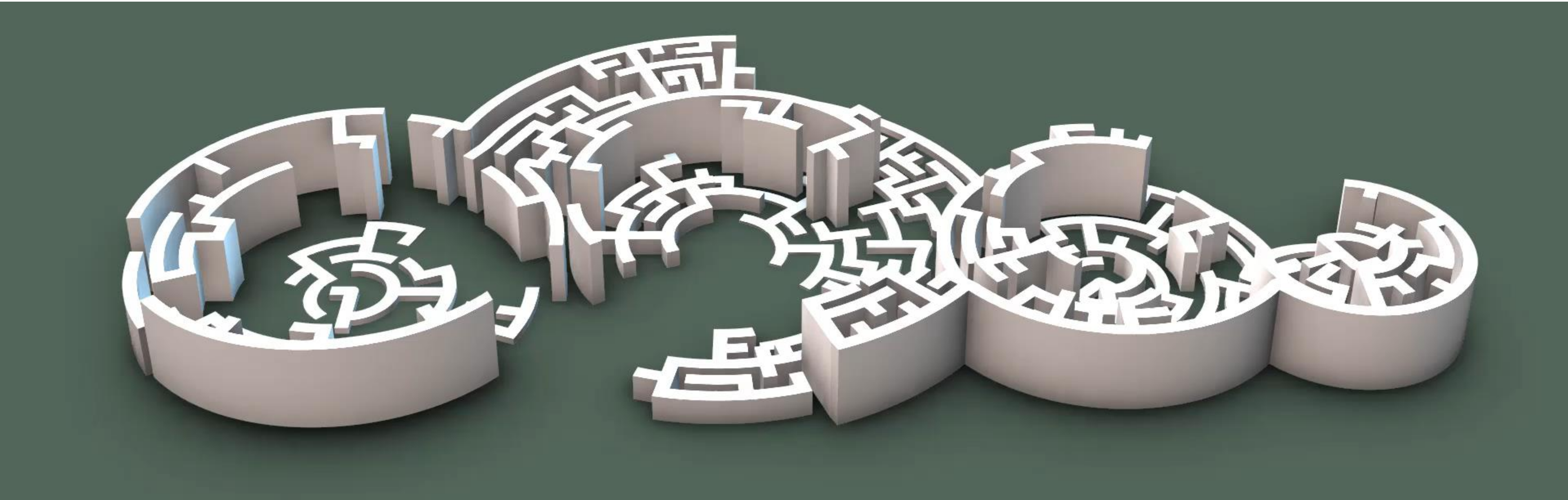
Dome9

- Extensive visibility for the ever-changing cloud assets with the ability to manage cloud native security controls
- Continuance compliance checks for governance and regulations, automatically remediation of misconfigurations and protecting the business
- Identity protection (IAM) preventing unauthorized access and account takeover.

CloudGuard Suite

Controller

- Provides adaptive security policy to the changes in your cloud assets.
- Enables a unified security policy over multi-cloud environments



CloudGuard Suite

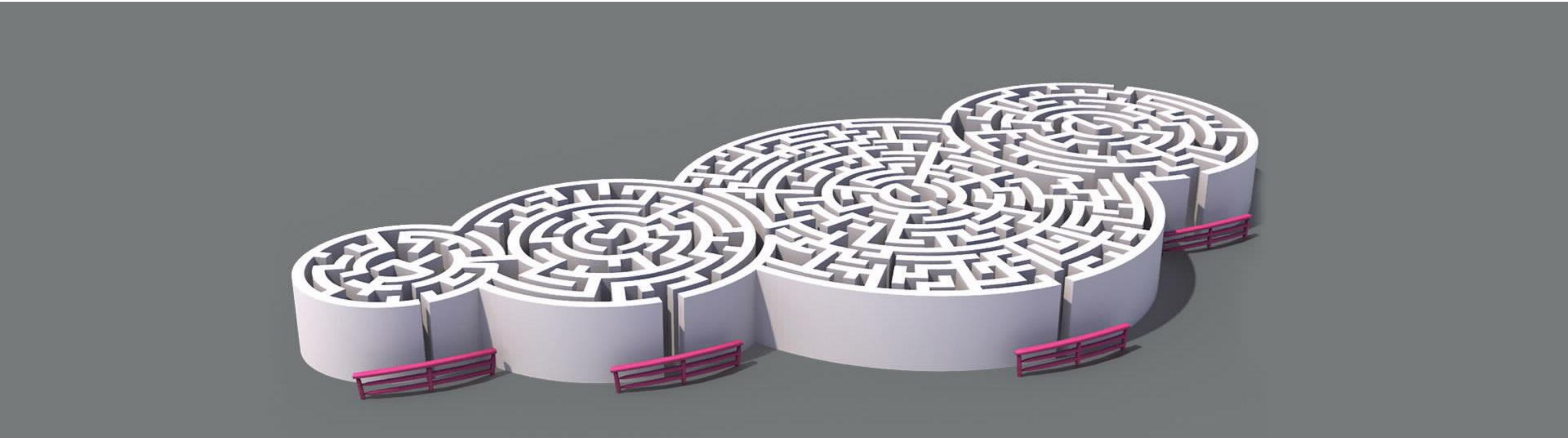
Check Point
SOFTWARE TECHNOLOGIES LTD.

Private Cloud

- Auto provisioned advanced threat prevention to control East-West traffic (lateral movements)
- Isolate infected machines with advanced security engines (like IPS, Anti-Bot, Zero-day protections and access control)

SaaS

- Protects cloud based applications malicious files and links.
- Prevent unauthorized access to services, using transparent, strong authentication to block account hijacks.
- Stop sophisticated emails attacks and email spoofing.



Over 4000 Customers have selected Check Point CloudGuard

- Comprehensive Security and Compliance for Multi and Hybrid Cloud Environments

Xero Completes and Secures Its Cloud Migration While Transforming Its Security Culture

https://www.checkpoint.com/customer-stories/xero/

Call to action



1 Design
Agile
Best practices

2 Operate
Adaptive Policy &
Continuous Compliance

3 Orchestrate
Security Orchestration

To Summarize

- Cloud is here & getting breached – use the most advanced threat prevention for cloud workloads
- Cloud assets are constantly changing - choose a partner that uses cloud native security controls for extensive visibility
- Misconfigurations are a real problem – choose a partner with real-time compliance checks to prevent misconfigurations
- Workloads are always changing – choose a partner that gives you adaptive security policy for those workloads
- Real customers have multiple clouds – choose a partner with multi-cloud support managed in a single pane of glass

Thank You

Please contact me with any

questions:

edumas@checkpoint.com